

# Measurement of information technology governance capability level: a case study of PT Bank BBS

Punto Widharto<sup>1</sup>, Zaldy Suhatman<sup>2</sup>, Rizal Fathoni Aji<sup>1</sup>

<sup>1</sup>Department of Computer Science, Faculty of Computer Science, Universitas Indonesia, Jakarta, Indonesia

<sup>2</sup>Department of Accounting, Faculty of Economy, Universitas Pamulang, Tangerang, Indonesia

## Article Info

### Article history:

Received Mar 04, 2021

Revised Feb 05, 2022

Accepted Feb 17, 2022

### Keywords:

COBIT

IS/IT management

IT governance

Performance management

## ABSTRACT

The very close involvement of technology in the banking industry makes almost all banking activities and products currently dependent on information technology (IT). PT BPRS Bhakti Sumekar (PT BBS Bank) is one of the banks that realizes the importance of IT in the digital era and has included IT as part of the company's strategic plan. The company states that compliance with regulations, best practices, and standards is key to a successful IT implementation. In this study, the measurement of the capability level of corporate IT governance was conducted to determine what IT priorities were based on the company's strategic objectives and what recommendations could be given based on best practices to improve IT services in support of the company's strategic goals. The framework to be used is control objective for information and related technology (COBIT); the most widely used framework suitable for service-oriented organizations. The results of research using COBIT 2019 show how IT governance is needed by the company and what should be prioritized. The measurement results found that there is still a gap between management's expectations and the current level of capability and provide recommendations on what companies need to improve performance in order to meet expectations.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Punto Widharto

Department of Computer Science, Faculty of Computer Science, Universitas Indonesia

Jl. Salemba Raya No. 4, Kec. Senen, Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10430, Indonesia

Email: punto.widharto@ui.ac.id

## 1. INTRODUCTION

The involvement of technology in the banking industry is tightly connected. Almost all banking activities and products currently depend on information technology (IT). A survey conducted by PricewaterhouseCoopers (PwC) in 2018 on 65 respondents from 51 banks in Indonesia regarding the bank business transformation plan in the next 3-5 years, shown that the highest percentage of survey results is 43%, which includes plans to invest in technology for business transformation [1]. PT BPRS Bhakti Sumekar (PT BBS Bank) is one of the banks that consists of a digital strategy into its strategic plan, aiming to digitize business processes towards service excellence. The digitization of companies' processes is carried out almost in the business sector and bank operations; the generous spirit of digitalization has made companies strongly dependent on technology and information systems. In the company business plan document (RBB), it is stated that the business strategy and company information technology strategy that is in harmony is needed for optimal IT implementation. IT is required to meet the availability of services and information, have an information system oriented to the needs of stakeholders, and have quality human resources. To meet its needs and align IT with its corporate strategy in the bank's business plan

(In Indonesian “*Rencana Bisnis Bank*” (RBB)), an IT-related strategic plan is drawn up as outlined in the information technology strategic plan (In Indonesian “*Rencana Strategis Teknologi Informasi*” (RSTI)).

According to the RSTI 2020-2022, it is said that to meet the demands of upholding the company's strategic plan, commitment and coordination of all division heads and division members is required, training for IT staff, asset maintenance, compliance with regulations, best practices, architecture and standards that have been prepared. However, based on the interviews with several parties from the business and operational departments, IT-related needs, and challenges were found. The problems raised in the interview were then used as the basis for further research on internal documents with the aim of validating the suitability of the informants' statements. The results were several findings that supported the statements of the informants. IT-related problems that arise are obstacles in implementing strategies to achieve company goals. This raises a gap between expectations from the company for IT support to achieve company goals, and it can be said that IT management has not reached the target. One of the root causes that cause management to have not reached the target is the absence of measurement of the level of IT governance capability, so it is not known what the level of IT governance in the company is currently and what improvements should be made. IT governance Institute stated that the failure to implement according to targets or agreements, poor efficiency, and the company's core processes are problems that arise from the ineffective IT governance in the organization [2]. This research will conduct a deeper study and focus on this problem with the formulation of research questions, "what is the level of IT service governance capability at PT BBS Bank?".

The definition of IT governance is the responsibility of the executive and the board of directors, and consists of leadership, organizational structures, and processes that ensure that corporate IT supports and expands organizational strategy and goals [2]. Good IT governance can provide benefits in the form of alignment of IT with company business objectives and is important because many studies have shown a correlation between the alignment of IT and business with company performance [3]. Effective IT governance requires IT frameworks that are well-designed, easy to understand, and have transparent mechanisms [4]. The IT framework is a series of processes, procedures, and policies that enable organizations to measure, monitor, and evaluate their situation against predetermined factors, criteria, or benchmarks [2]. In IT governance, there are many frameworks that can be used. According to some literature that has been collected, control objectives for information technologies (COBIT) is the most widely used framework; the reason for using COBIT is because COBIT is the most widely used and accepted framework for IT governance.

COBIT has been widely accepted as a framework that can bring together various frameworks and other best practices, such as information technology infrastructure library (ITIL), international organization for standardization (ISO) 38500, and ISO 17799 [5]-[7]. Research conducted by Leketi and Raborife states that COBIT is the most widely used and popular framework around the world [8]. It is also said that this framework is also effective in providing guidance to boards and bank management. Leketi and Raborife [8] also said that the COBIT framework is the best framework to use in industries related to service delivery, including the banking industry, which is service-oriented and must maintain high standards of satisfaction. Other studies that recommend COBIT state that COBIT provides a comprehensive framework that assists companies in achieving their goals for corporate IT governance and management and provides a structure that uniform to implement, understand and evaluate the performance, capabilities, and risks of IT with the main objective of meeting business requirements [9]-[11].

COBIT 2019 is a governance framework issued by the information systems audit and control association (ISACA) which is an improvement from the previous version, namely COBIT 5. COBIT 2019 defines design components and factors to create and maintain a governance system that best suits the company and is recognized globally as one of the corporate governance frameworks for information technology. At COBIT 2019, there are seven components to build and maintain a governance system: processes, organizational structure, policies and procedures, information flow, culture and behaviour, skills, and infrastructure. COBIT 2019 also addresses governance issues by grouping the relevant governance components into governance objectives and management that can be managed to the required level of capability, taking into account design factors according to company needs. COBIT 2019 has a set of governance called COBIT core, which consists of 5 domains and 40 governance processes [12], [13].

At COBIT 2019, a solution was introduced to adjust IT governance to company needs called the COBIT 2019 design factor. This design factor is a factor that can influence the governance design of a company to support its success in the use of information technology. Overall, there are 11 factors contained in the 2019 COBIT factor design. The combination of an assessment of these eleven factors will produce a focus area of IT governance in the organization. Although there are many factors in making organizational governance designs, the main factors that influence the most are the enterprise strategy, enterprise goals, risk profile, and IT-related issues, while other factors are optional [14].

The measurement of the IT capability value will be carried out using COBIT performance management (CPM), which is used to measure the capability level. Capability level is the level of capability

of each governance practice, which is a part of governance objectives given when activities on governance practice have been achieved. The assessment rating at the ability level uses the not partially largely fully (NPLF) model (not - less than 15%, partially - between 15% and 50%, largely - between 50% and 85%, fully - between 85% and 100%) based on the results of the assessment for each activity [15]. The assessment for capability has a rating of 0 (zero) to 5 (five), but at COBIT 2019 there is no activity in the practice area with a value of 0 (zero) and 1 (one), so it is difficult to determine the value of a practice area that does not reach a capability score of 2 (two). The assessment procedure to be used to overcome this problem is to use a procedure based on research conducted by [15] to provide more flexibility and realizing that not all processes or activities are critical [14]. The details of the proposed measurement procedure are as follows:

- 1) For each listed process, the desired rating (N, P, L, F) must be assigned to each activity at level 2. Further, the organization should proceed as follows:
  - a. If all level 2 activities in each practice have been rated L or F, this process meets the level 2 requirements at least.
  - b. If there is a level 2 activity across all process practices that have been rated N or P, it is considered to be at level 2 [16].
- 2) For each process on the list that has achieved capability level 2 (two), the desired rating (N, P, L, or F) must be assigned to each activity at level 3 (three). Then, the organization should proceed as follows:
  - a. If all level 3 activities in each practice have been rated L or F, the process has, at least, met the level 3 requirement.
  - b. If there are level 3 activities across all process practices that have been rated N or P, then assign level 2 to the process.

In this case study, the organization has IT policies and guidelines made based on the reference of the Financial Services Authority (In Indonesian “*Otoritas Jasa Keuangan*” (OJK)) regulation POJK No. 38/POJK.03.2016 about application of risk management in the use of information technology by commercial banks (In Indonesian “*Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*”) [17] and SEOJK No. 21/SEOJK.03/2017 about application of risk management in the use of information technology by commercial banks (In Indonesian “*Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*”) [18]. OJK is an institution that acts as a regulator and supervises all activities in the financial sector. Therefore, measuring the level of maturity in this case study will also consider the two regulations as a reference.

## 2. RESEARCH METHOD

This study uses a qualitative research methodology that is suitable for researching problems that are not yet clear and can help researchers understand the phenomena that occur more broadly [19]. This research takes an organization as a place of research. Therefore, this research is classified into a case study, where the research scope is limited to a particular organization or community. Collecting data in research is through interviews with parties involved in the object of research, coupled with observations in the work environment, documentation, and organizational reports. The process flow of this research can be seen in Figure 1.

The research started from determining the topic and collecting related data, followed by identifying and formulating problems in determining the focus of the research objectives. Then conducted a literature study from previous research and determined the framework to be used. The results of the literature study are in the form of designing an IT governance system according to organizational needs. Based on this design, measurement of the maturity level of IT governance in the organization is carried out, starting with interviewing the persons who are accountable for the management objectives being evaluated. For example, to measure governance regarding incident management, the interviewee is the head of the IT solution management department who is responsible for the helpdesk, monitoring the production area, and managing problems. After that, the collection and review of related data are carried out to look for evidence related to the objective being studied to measure the level of maturity. Measurement of management expectations is carried out by conducting interviews and discussing with the head of the IT group. The gap between the measurement results and expectations is then used to provide recommendations to increase the level of organizational capability.

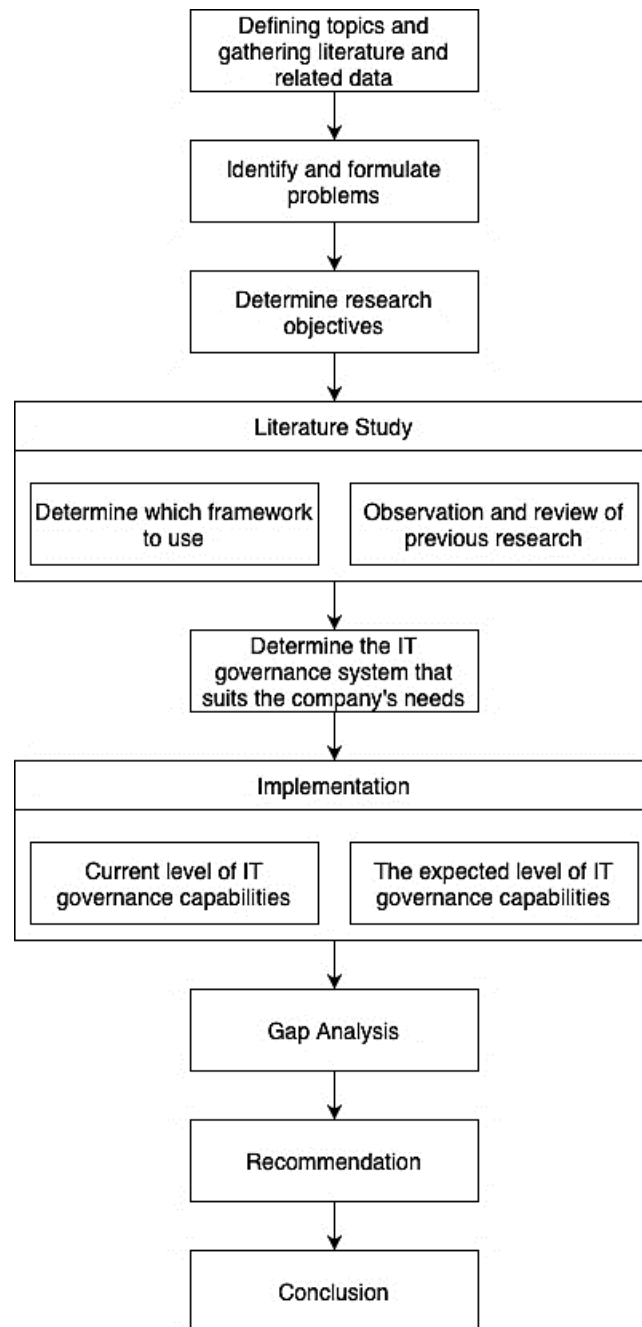


Figure 1. Research flow

### 3. RESULTS AND ANALYSIS

The results of the analysis are divided into two sub-categories, the first is the measurement of design factors to identify priority objectives in the IT governance system based on organizational needs, and the second is the measurement of the level of IT governance capabilities in the organization. In the first category, an evaluation is carried out by identifying IT priorities to determine their alignment with company goals. Furthermore, in the second category, measurements of the level of existing IT governance capabilities in the company are carried out.

#### 3.1. Identify IT priorities

The IT governance evaluation process begins with identifying IT priorities to ensure that the objectives to be evaluated are IT activities that are aligned with company goals. In identifying IT priorities, there are several assessments based on factors that affect the priority of the governance system, which is

called the design factor. Assessment can give positive and negative results based on the level of importance, based on the value that has been determined by the COBIT. In the corporate strategy design factor, which is one of the factors that influence the design of governance, taking into account the current company strategy, namely digitizing business processes towards service excellence and the company roadmap in 2021, becoming the leading sharia banking in services and ops excellence, the client service/stability strategy pattern has the highest value followed by growth/acquisition Table 1.

Table 1. Company strategy based on priority

Value	Importance (1-5)	Baseline
Growth/acquisition	4	3
Innovation/differentiation	3	3
Cost leadership	2	3
Client service/stability	5	3

The next identification is based on the enterprise goal design factor. In this design factor, the business goals that are the priority of the company are mapped into the enterprise goals that are in COBIT 2019 enterprise goal design factor. The analysis found that improving services, improving product and service quality, and optimizing business processes while still paying attention to risks and compliance with regulations are the top priorities in companies today. Based on the results of this analysis, the mapping was carried out into the enterprise goals at COBIT 2019, and it was determined that EG05, EG06, EG02, EG03, and EG08 were the enterprise goals that were the top priority Table 2.

Table 2. Company enterprise goal based on COBIT 2019

Value	Importance (1-5)	Baseline
EG01 - portfolio of competitive products and services	3	3
EG02 - managed business risk	4	3
EG03 - compliance with external laws and regulations	4	3
EG04 - quality of financial information	3	3
EG05 - customer-oriented service culture	5	3
EG06 - business-service continuity and availability	5	3
EG07 - quality of management information	2	3
EG08 - optimization of internal business process functionality	4	3
EG09 - optimization of business process costs	2	3
EG10 - staff skills, motivation and productivity	3	3
EG11 - compliance with internal policies	3	3
EG12 - managed digital transformation programs	2	3
EG13 - product and business innovation	3	3

The third factor in determining an IT governance system is based on the IT risk profile in the organization. In determining the design factor based on this risk profile, mapping is carried out between the IT risk profiles compiled by the organization and the risk categories in COBIT 2019. The results of the risk profile mapping are shown in Table 3. Several risks have a high rating, especially software failure and data management & information, which has a high impact and likelihood. The reason for the high probability of software failure is the existence of audit findings, while in data and information management is due to delays in reporting due to the time-consuming process of preparing reports.

The fourth factor that influences the design of an IT governance system is based on issues or problems that exist in IT in the organization. In the analysis, it was found that the main issues related to IT were the number of IT-related incidents in the organization, especially tickets to the helpdesk regarding application failures and audit findings related to application failures. Management believes that the lack of personnel to handle the problems is the cause of the emergence of these issues, apart from technical problems. This fourth factor is referred to as the IT-related issue design factor at COBIT 2019, and the priority for organizations is:

- Significant IT-related incidents, such as data loss, security breaches, project failure, and application errors, linked to IT.
- Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems.
- Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction.

Based on the assessment of the factors that form the basis for the formulation of IT governance design factors and assisted by the COBIT 2019 design toolkit, the value of priority governance and IT management objectives in the organization is obtained as shown in Figure 2. From the results of the assessment, six objectives were selected with the highest scores to measure their level of ability, namely APO011 - managed quality, APO012 - managed risk, APO013 - managed security, BAI06 - managed IT change, DSS02 - managed service request and incidents, DSS03 - managed problems. These six objectives are objectives that need higher priority because of their importance to the corporate governance system according to the results of the assessment.

Table 3. IT risk profile based on COBIT 2019

Risk scenario category	Impact (1-5)	Likelihood	Risk rating	Baseline
IT investment decision making, portfolio definition & maintenance	3	2	6	9
Program and projects life cycle management	3	2	6	9
IT costs and oversight	3	2	6	9
IT expertise, skills & behaviour	4	2	8	9
Enterprise/IT architecture	3	2	6	9
IT operational infrastructure incidents	5	2	10	9
Unauthorized actions	3	2	6	9
Software adoption/usage problems	3	3	9	9
Hardware incidents	5	2	10	9
Software failures	4	3	12	9
Logical attacks (hacking and malware)	5	2	10	9
Third-party/supplier incidents	4	2	8	9
Noncompliance	3	2	6	9
Geopolitical issues	1	1	1	9
Industrial action	1	1	1	9
Acts of nature	2	1	2	9
Technology-based innovation	3	2	6	9
Environmental	2	1	2	9
Data & information management	4	3	12	9

### 3.2. Measuring the level of IT governance capabilities

As an illustration of measuring the level of IT governance capability, one sample of measurement results from the APO11 (managed quality) will be taken. APO11's management objective is to ensure the consistent delivery of technology solutions and services to meet the quality required by the company and meet the needs of stakeholders. The results of the analysis show that there are quality standards in the organization, and evidence of the application of these quality standards is found in development project documents in the form of development documentation, testing documentation, and user acceptance documents. However, there is no evidence that there have been regular reviews of existing quality control systems and reviews of user expectations and feedback about the organization's quality management system. There was also a 7% increase in the improvement and enhancement projects from 2019 to 2020, indicating that the effectiveness and performance of the existing quality management system have not been adequately reviewed.

Based on the analysis, it is known that the level of ability of APO11 (managed quality) in the organization has now reached level 2 on Table 4. The level of capability is obtained by assessing every practice that exists in APO11 management practices, for example in management practice APO11.01, there are 3 practices that must be fulfilled so that level 3 capabilities can be met, as well as in management practice APO11.03, while in management practice APO11.02 there are 4 practices that must be fulfilled in order for the level 3 capability to be fulfilled, and so on. In Table 4 it can be seen that all the practices required to reach capability level 2 have been successfully achieved. In the practices needed to achieve capability level 3, it can be seen that management practices APO11.01 and APO11.02 managed to get a full score, which means that all the practices needed to achieve capability level 3 have been achieved, while in APO11.03 management practices for capability level 3 only scored 67%, this is because only 2 out of 3 practices were successfully achieved.

Meanwhile, according to policies and regulations, activities related to APO11 (managed quality) in an organization can be said to have met the applicable regulations. This is because the current regulations (POJK No. 38/POJK.03.2016 and SEOJK No. 21/SEOJK.03/2017) do not provide detailed guidance on the implementation of IT governance. Current regulations only provide IT governance guidelines for managing IT risk in general (for example, all system development and corrections must be documented, there should be trials such as unit tests, system integration tests, and user acceptance tests before implementation), whereas detailed procedures and the management of the practice is left to each organization.

## Governance and Management Objectives Importance

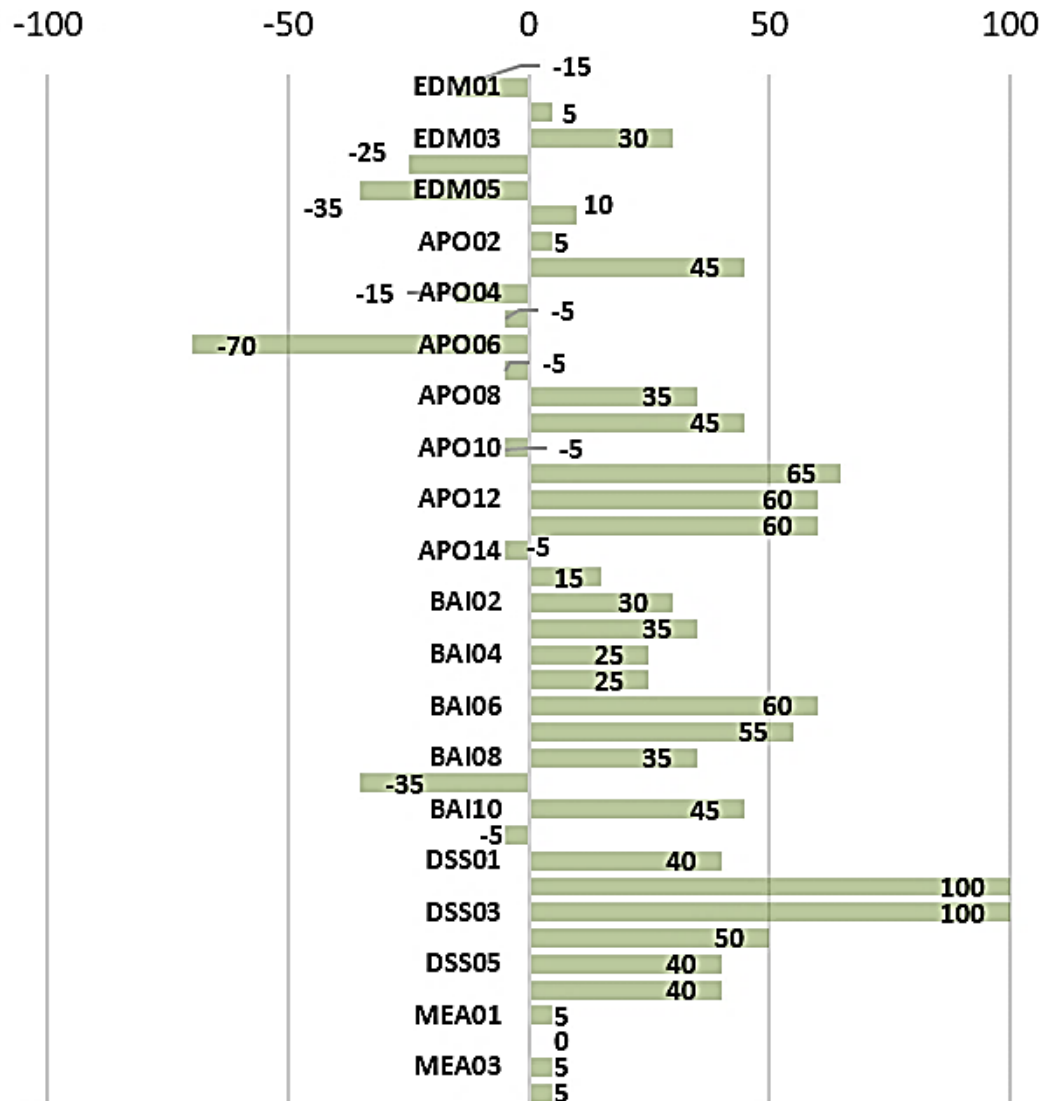


Figure 2. The result of COBIT 2019 design factor analysis

Table 4. APO11 objective measurement results

Capability Level	Level 2				Level 3		
APO11	APO11.03	APO11.05	APO11.01	APO11.02	APO11.03	APO11.04	APO11.05
Rating by criteria	100%	100%	100%	100%	67%	0%	33%
Capability level achieved	F	F	F	F	L	N	P

Overall, the average IT governance capability level score in the organization is at level two except for APO13, which is at level 3. Meanwhile, based on the results of interviews, to optimally support the IT strategic plan for the 2020-2022 period, management expects that the IT governance capability level in the organization can reach level 4 on Figure 3. This target is set by considering that the increase in the capability level must be done in stages, with level 4 expected to be achieved by 2022.

### Existing vs Expected Performance

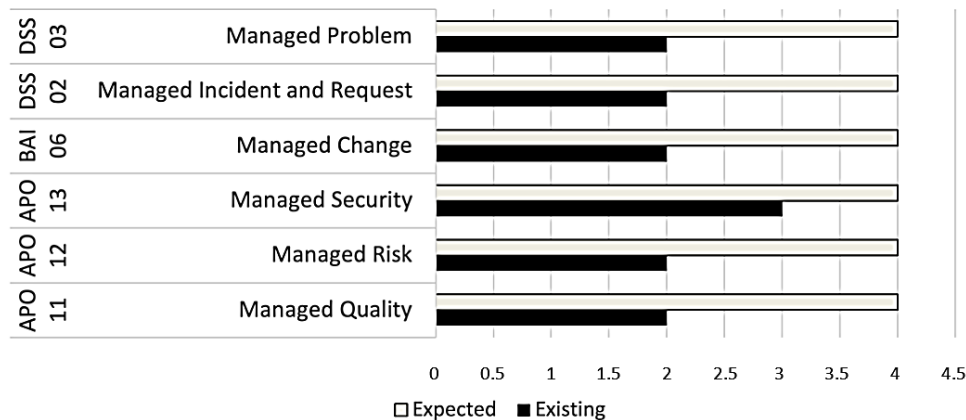


Figure 3. The gap between the current assessment results and expectations

### 3.3. Recommendation

In the management objective of APO11, practices that must be improved in order to achieve capability level 4 are:

- APO11.01 - establish a quality management system (QMS): periodic review and supervision of conformity of quality management to acceptance criteria.
- APO11.02 - focus quality management on customers: periodically reviewing the views and feedback from users on the business processes and solutions provided.
- APO11.03 - manage quality standards, practices and procedures and integrate quality management into key processes and solutions: effectively communicate quality standards, supervise the quality of data, and periodically review the efficiency and effectiveness of specific quality control processes.
- APO11.04 - perform quality monitoring, control and reviews: conducting a quality review of the processes and solutions given. Observe measures of success to align with quality objectives. Ensure the person in charge of the process periodically reviews quality performance with the specified metrics and analyzes the overall performance.
- APO11.05 - maintain continuous improvement: Identify recurring quality defects, determine the root of the problem and evaluate their impact. Provide training to employees on methods and tools for continuous improvement and conduct quality review results from comparison against past data, industry guidelines, and standards.

At COBIT 2019, best practices and frameworks related to management practice have been mapped as guidelines. Recommendations to increase the level of capability in APO11 are to use best practices guidelines and frameworks related to APO11 management practices, namely project management body of knowledge (PMBOK) sixth edition and national institute of standards and technology (NIST) - framework for improving critical infrastructure cybersecurity v1.1, April 2018.

- APO11.01 - establish a quality management system (QMS); In the current organizational guidelines and standard procedure documents, although quality management planning has been defined by the framework, in its implementation, there has been no periodic review of the conformity of the quality management system with user acceptance criteria. Recommendations for improving this activity are to conduct periodic reviews of all project documents and ensure that there are parameters that can be used as a measure of quality management. Through a review of these activities and documentation, it will be possible to determine the level of acceptance of the quality management system. Besides that, it is also recommended to get an overview of the business processes and solutions delivered by IT by holding regular project progress meetings. In this management practice, COBIT recommends using the guidelines from PMBOK 6<sup>th</sup> edition [20].
- APO11.02 - focus quality management on customers. Conduct periodic reviews regarding whether the business processes carried out are appropriate and meet user expectations.
- APO11.03 - manage quality standards, practices, and procedures and integrate quality management into critical processes and solutions. The current standard procedure documents require business requirement document (BRD), case report form (CRF), and testing forms to maintain quality management, but there has been no periodic training on quality management approaches. Based on this,



it is recommended that a standard operating procedure (SOP) or guide be made in managing quality management using the framework of PMBOK 6<sup>th</sup> edition [20].

- APO11.04 - perform quality monitoring, control, and reviews. In the measurement results of APO11.04 management practice, procedures for monitoring and quality control, control activities carried out only revolve around reports containing the project's status and timeline. Based on this, it is recommended to apply the framework of PMBOK 6th edition regarding quality control, for example, based on data collected from management practices APO11.01, APO11.03, and change requests, perform a performance review analysis and root-cause analysis of system failures/defects.
- APO11.05 - maintain continuous improvement. In the results of measuring management practice APO11.05, a platform has been created to share good practices and capture information about defects and errors to be used as lessons in the future, but there have been no quality defect identification activities, analysis, and valuation of impacts and results, besides that there are also no benchmarking activities resulting from quality reviews against previous data, industry guidelines, and standards from similar companies. Based on this, it is recommended to apply the framework from NIST - framework for improving critical infrastructure cybersecurity v1.1, April 2018 [21].

Regardless of the management objectives that were sampled, all management objectives measured in this study were given recommendations and guidelines to improve the capabilities of their management practices. In summary, what management practices need to be improved in each measured process and guidelines that can be used to increase the level of capability in all measured management objectives are mapped in Table 5. The related guidelines given here are best practice guidelines taken from various organizations.

Table 5. Related guidelines recommendation

Management objective	Management practice	Related guidelines
APO11 - managed quality	APO11.01	PMBOK guide sixth edition, 2017 [20]
	APO11.02	PMBOK guide sixth edition, 2017 [20]
	APO11.03	PMBOK guide sixth edition, 2017 [20]
	APO11.04	PMBOK guide sixth edition, 2017 [20]
	APO11.05	NIST framework for improving DE. DP detection processes critical Infrastructure cybersecurity v1.1, April 2018 [21]
APO12 - managed risk	APO12.01	ISO/IEC 27005, NIST SP 800-37, revision 2 (draft), May 2018 [22]
	APO12.02	NIST SP 800-53, revision 5 (draft), August 2017 [22]
	APO12.03	NIST SP 800-53, revision 5 (draft), August 2017 [22]
	APO12.04	NIST SP 800-53, revision 5 (draft), August 2017 [22]
	APO12.05	HITRUST CSF version 9
	APO12.06	ISO/IEC 27005, NIST SP 800-53, revision 5 (draft), August 2017 [22]
APO13 - managed security	APO13.02	NIST SP 800-37, revision 2 (draft), May 2018, national institute of standards and technology special publication 800-53, revision 5 (draft) [22]
	APO13.03	NIST SP 800-37, revision 2 (draft), May 2018 [22]
BAI06 - managed IT changes	BAI06.01	ITIL V3: service transition, 2011 [23]
	BAI06.02	ITIL V3: service transition, 2011 [23]
	BAI06.03	ITIL V3: service transition, 2011 [23]
	BAI06.04	ITIL V3: service transition, 2011 [23]
DSS02 - managed service requests and incidents	DSS02.01	ISO/IEC 20000-1:2011 [24]
	DSS02.02	ISO/IEC 20000-1:2011 [24]
	DSS02.06	ISO/IEC 20000-1:2011 [24], ITIL V3: service operation, 2011 [25]
	DSS02.07	ISO/IEC 20000-1:2011 [24]
DSS03 - managed problems	DSS03.02	ITIL V3: service operation, 2011
	DSS03.03	ITIL V3: service operation, 2011
	DSS03.04	ITIL V3: service operation, 2011
	DSS03.05	ITIL V3: service operation, 2011

#### 4. CONCLUSION

COBIT 2019 currently has 40 objective management components to determine current IT governance priorities in the organization. The COBIT 2019 design factor tool provided by ISACA as a tool that helps facilitate prioritization is very useful in providing an idea of what a governance system design will look like in accordance with company conditions. In this study, it was found that using the 2019 COBIT design factor, management objectives APO11, APO12, APO13, BAI06, DSS02, and DSS03 are important

objectives and are a priority in the corporate governance system. In measuring the level of IT governance capability in the objective management, it can be seen that the level of governance capability in the organization is at level 2, below the expectations of management who want the ability level to be at level 4. Even so, the organization can be said to have complied with existing regulations because the current regulations do not provide detailed guidelines and rules regarding the implementation of IT governance in organizations. Based on the measurement results compared to management's expectations, it is recommended to make improvements to activities with the best practice guidelines and frameworks suggested by COBIT.

In further research using COBIT 2019 in the same industrial sector, it is recommended that research be carried out on the company's organizational structure to see the relationship between the current level of IT governance capability values and the structure and responsibilities of each person in the company. Furthermore, although in the current case study, the company received a capability score of two, the organization was deemed to comply with the rules of the regulation. Based on this, it is recommended that a study be carried out regarding the adequacy of regulatory rules in the current banking industry sector and whether organizations in the banking sector should use other frameworks such as COBIT 2019 as a compliment.




## REFERENCES

- [1] P. Widharto, A. I. Pandesenda, A. N. Yahya, E. A. Sukma, M. R. Shihab, and B. Ranti, "Digital Transformation of Indonesia Banking Institution: Case Study of PT. BRI Syariah," *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, 2020, pp. 44-50, doi: 10.1109/ICITSI50517.2020.9264935.
- [2] IT Governance Institute, *Board Briefing on IT Governance - 2nd Edition*, California, 2003. [Online]. Available: [https://eventosfehos.com.br/2017/material/sao\\_paulo/ti/jose/ITGI-Instrucoes-de-Governanca-de-TI-para-a-Alta-Administracao.pdf](https://eventosfehos.com.br/2017/material/sao_paulo/ti/jose/ITGI-Instrucoes-de-Governanca-de-TI-para-a-Alta-Administracao.pdf)
- [3] S. D. Haes and W. V. Grembergen, *Enterprise governance of information technology: Achieving strategic alignment and value*, Boston, MA: Springer, 2009, doi: 10.1007/978-0-387-84882-2.
- [4] J. W. Ross and P. Weill, *IT Governance How Top Performers Manage IT Decisions Rights for Superior Results*, Harvard Business School Press, Jun. 2004. [Online]. Available: [https://www.researchgate.net/publication/236973378\\_IT\\_Governance\\_How\\_Top\\_Performers\\_Manage\\_IT\\_Decision\\_Rights\\_for\\_Superior\\_Results](https://www.researchgate.net/publication/236973378_IT_Governance_How_Top_Performers_Manage_IT_Decision_Rights_for_Superior_Results).
- [5] A. Joshi, L. Bollen, H. Hassink, S. de Haes, and W. V. Grembergen, "Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role," *Information and Management*, vol. 55, no. 3, pp. 368–380, 2018, doi: 10.1016/j.im.2017.09.003.
- [6] A. Cartledge *et al.*, "ITSMF: An Introductory Overview of ITIL 2011," In *An Introductory Overview of ITIL® 2011, 2012*. [Online]. Available: <https://www.educore.com.tr/downloads/itiloverview.pdf>
- [7] G. Hardy and J. Heschl, *Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for business benefit*, USA: IT Governance Institute 2008. [Online]. Available: <https://silo.tips/download/aligning-cobit-41-itil-v3-and-iso-iec-for-business-benefit-a-management-briefing>
- [8] M. Leketi and M. Raborife, "IT Governance Frameworks and their Impact on Strategic Alignment in the South African Banking Industry," *2019 IST-Africa Week Conference (IST-Africa)*, 2019, pp. 1-9, doi: 10.23919/ISTAfrica.2019.8764872.
- [9] M. R. Safari and Q. Jiang, "The theory and practice of IT governance maturity and strategies alignment: Evidence from banking industry," *Journal of Global Information Management*, vol. 26, no. 2, pp. 127–146, Feb. 2018, doi: 10.4018/JGIM.2018040106.
- [10] M. Jäntti and V. Hotti, "Defining the relationships between IT service management and IT service governance," *Information Technology and Management*, vol. 17, no. 2, pp. 141–150, 2016, doi: 10.1007/s10799-015-0239-z.
- [11] N. Legowo and Christian, "Evaluation of Governance Information System Using Framework Cobit 5 in Banking Company," *2019 International Conference on Sustainable Engineering and Creative Computing (ICSECC)*, 2019, pp. 281-286, doi: 10.1109/ICSECC.2019.8907123.
- [12] Information Systems Audit and Control Association, *COBIT 2019 Framework Introduction and methodology*, 2018.
- [13] Information Systems Audit and Control Association, *COBIT 2019 Framework Governance and Management Objective*, 2018.
- [14] Information Systems Audit and Control Association, *COBIT 2019 Designing an Information and Technology Governance Solution*, 2018.
- [15] J. S. Neto, R. Almeida, and M. M. D. Silva, "Defining Target Capability Levels in COBIT 2019: A Proposal for Refinement," *Universidade Católica de Brasília*, Mar. 2019, doi: 10.13140/RG.2.2.19359.20647.
- [16] V. S. Kasma, S. Sutikno, and K. Surendro, "Design of e-Government Security Governance System Using COBIT 2019: (Trial Implementation in Badan XYZ)," *2019 International Conference on ICT for Smart Society (ICISS)*, 2019, pp. 1-6, doi: 10.1109/ICISS48059.2019.8969808.
- [17] Otoritas Jasa Keuangan Republik Indonesia, "POJK No. 38/POJK.03/2016," *Application of Risk Management in the Use of Information Technology by Commercial Banks* (In Indonesian "Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum"), 2016. [Online]. Available: <https://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%20MRTL.pdf>
- [18] Otoritas Jasa Keuangan Republik Indonesia, "SEOJK No. 21/SEOJK.03/2017," *Application of Risk Management in the Use of Information Technology by Commercial Banks* (In Indonesian "Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum"), 2017. [Online]. Available: <https://www.ojk.go.id/id/kanal/perbankan/regulasi/surat-edaran-ojk/Documents/SAL%20SEOJK%2021%20-%20MRTL.pdf>
- [19] J. Recker, "Scientific Research in Information Systems," *A Beginner's Guide*, 2013. [Online]. Available: <https://link.springer.com/book/10.1007/978-3-642-30048-6>.
- [20] Project Management Institute, *A guide to the project management body of knowledge (PMBOK guide), PMBOK Guide 6<sup>th</sup> Edition*, 2017.
- [21] M. Barrett, "Framework for improving critical infrastructure cybersecurity," *Proceedings of the Annual ISA Analysis Division Symposium*, 2018, vol. 535, pp. 9–25. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf>




- [22] NIST, "Risk management framework for information systems and organizations," *NIST Special Publication - 800 series*, p. 183, 2018. [Online]. Available: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>
- [23] S. Rance, "ITIL Service Transition," *In the Stationery Office*, 2011.
- [24] International Organization for Standardization, "INTERNATIONAL STANDARD ISO/IEC 20000-1:2018 - Information technology - Service management," 2018. [Online]. Available: <https://www.iso.org/standard/70636.html>.
- [25] R. Steinberg, "ITIL Service Operation," *In the Stationery Office*, 2011.

## BIOGRAPHIES OF AUTHORS






**Punto Widharto**    received a master's degree (M.T.I) from the University of Indonesia, Jakarta, Indonesia. Received a bachelor's degree in computer science from NIIT college. His areas of research are computer networks and IT governance. He currently works as a Policy and Security Standards Team Leader at Bank Syariah Indonesia. He can be contacted at email: [punto.widharto@gmail.com](mailto:punto.widharto@gmail.com).



**Zaldy Suhatman**    received a master's degree (MBA) from the Bandung Institute of Technology, Bandung, Indonesia. Received a bachelor's degree in economics from the University of Riau, Riau, Indonesia. His areas of research are accounting information systems, Islamic economics, Islamic banking. He currently works as a lecturer at Pamulang University and is the head of the IT Implementation and Monitoring department at Bank Syariah Indonesia. He can be contacted at email: [Zaldy@unpam.ac.id](mailto:Zaldy@unpam.ac.id).



**Dr. Rizal Fathoni Aji**    received a doctorate in computer science at the university of Indonesia, Jakarta, Indonesia. Received a master's degree in computer science at the university of Indonesia, Jakarta, Indonesia. His areas of research are computer networks and information security. Currently he works as a lecturer and IT Manager at the university of Indonesia. He can be contacted at email: [rizal@cs.ui.ac.id](mailto:rizal@cs.ui.ac.id).